Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 9 (2014) pp. 027-033
© MIR Labs, www.mirlabs.net/jias/index.html

New Mathematical Modeling For Cryptography

A.P. Hiwarekar
Vidya Pratishthan's College of Engineering,
Vidyanagari, Bhigwan Road,Baramati,
(University of Pune)
Dist.Pune, Maharashtra, India, Pin-413133
Email-hiwarekaranil@gmail.com

Abstract : Information protection has been an important part of human life from ancient time. In computer society, information security becomes more and more important for humanity and new emerging technologies are developing in an endless stream. Cryptography is one of the most important techniques used for securing transmission of messages and protection of data. Examples includes, e-commerce; electronic communications such as mobile communications, sending private emails; business transactions; Pay-TV; transmitting financial information; security of ATM cards; computer passwords etc, which touches on many aspects of our daily lives. Cryptography provides privacy and security for the secret information by hiding it. It is done through mathematical technique.

Laplace transform has many applications in various fields here we discuss its new application to cryptography. This paper presents a new iterative method for cryptography, in which we apply successive Laplace transform of suitable function for encrypting the plain text and apply corresponding inverse Laplace transform for decryption. Generalization of the results is also obtained.

Encryption by Laplace Transform is resistance to nearly all types of attacks on symmetric encryption algorithms. There is flexibility in implementation of algorithms. One can implement the algorithms as per the application demands. We can find many application of encryption by Laplace Transform in banking, Security, One time password generation.

Key words: Cryptography, Data encryption, Applications to coding theory and cryptography, Algebraic coding theory; cryptography, Laplace Transforms.

1. Introduction

In Today's world, with increasing usage of computer networks and internet, the importance of network, computer and information security is obvious. To be secured, information needs to be protected from unauthorized access. Hence, data security has become a critical and imperative issue. One of the widely used approaches for information security is Cryptography. Cryptography, the mathematic of encryption, plays a vital role in many fields.

The fundamental objective of cryptography is to enable two people, to communicate over an insecure channel in such a way that an opponent cannot understand what is being said. Encryption is the process of obscuring information to make it unreadable without special knowledge. A cipher is an algorithm for performing encryption (and the reverse, decryption) a series of well-defined steps that can be followed as a procedure. The original information is known as plain text, and the encrypted form as cipher text. The cipher text message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it. Ciphers are usually parameterized by a piece of auxiliary information, called a key. The encrypting procedure is varied depending on the key which changes the detailed operation of the algorithm. Without the key, the cipher cannot be used to encrypt, or more importantly, to decrypt, [1, 2, 3, 5, 6, 7, 10, 11, 12]. Various techniques for cryptography are found in literature [1], [2], [3], [5], [12], [17], [18]. Mathematical technique using matrices for the same are found in Dhanorkar and Hiwarekar, [4]; Overbey,Traves and Wojdylo, [14]; Saeednia, [16]. In Naga Lakshmi, Ravi Kumar and Chandra Sekhar, [7]; Hiwarekar, [10] and [11]; Vyavahare, Bani Upmanayu; [21]; Sujitha, [19]; they encrypt a string by using series expansion of f(t) and its Laplace transform and the results for cryptanalysis found in Gupta and Mishra [9]. DNA secret writing using Laplace transform is found in Sukalyan and Moumita [20].

2. Definitions and Standard Results

Definition 2.1.: Plain text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to that message.

Definition 2.2.: When plain text message is codified using any suitable scheme, the resulting message is called as cipher text.

Definition 2.3.: Encryption transforms a plain text message into cipher text, whereas decryption transforms a cipher text message back into plain text. Every encryption and decryption process has two aspects: The algorithm and the key. The key is used for encryption and decryption that makes the process of cryptography secure. Here we require following results.

2.1. The Laplace Transform: If $f(t)$ is a function defined for all positive values of t, then the Laplace Transform of $f(t)$ is defined as

$$L\{f(t)\} = F(s) = \int_0^\infty e^{-st} f(t)dt, \tag{2.1}$$

provided that the integral exists. Here the parameter s is a real or complex number. The corresponding inverse Laplace transform is $L^{-1}\{F(s)\} = f(t)$, [6, 8, 13, 15].

2.2. Theorem: Laplace transform is a linear transform. That is, if

$$L\{f_1(t)\} = F_1(s), L\{f_2(t)\} = F_2(s), \cdots L\{f_n(t)\} = F_n(s), \tag{2.2}$$

then

$$\begin{aligned} &L\{c_1 f_1(t) + c_2 f_2(t) + \cdots c_n f_n(t)\} \\ &= c_1F_1(s) + c_2F_2(s) + \cdots + c_nF_n(s), \end{aligned} \tag{2.3}$$

where $c_1, c_2, \cdots, c_n$ are constants, [6, 8, 13, 15].

2.3. Some Standard Results of Laplace Transform:

In this paper we are assuming that all the considered functions are such that their Laplace transform exists. We are also assuming that N be the set of natural numbers. Here we consider following standard results of Laplace transform

1. $$\begin{aligned} &L\{\sinh kt\} = \frac{k}{s^2 - k^2}, \\ &L^{-1}\{\frac{k}{s^2 - k^2}\} = \sinh kt. \end{aligned} \tag{2.4}$$

2. $$L\{t^n\} = \frac{n!}{s^{n+1}}, \quad L^{-1}\{\frac{n!}{s^{n+1}}\} = t^n, \quad n \in N. \tag{2.5}$$

3 . $$\begin{aligned} &L\{t^n f(t)\} = \left(\frac{-d}{ds}\right)^n F(s), \\ &L^{-1}\{\left(\frac{-d}{ds}\right)^n F(s)\} = t^n f(t), \end{aligned} \tag{2.6}$$

[6, 8, 13, 15].

3. Main Results

3.1 Encryption

We consider standard expansion

$$\begin{aligned} \sinh rt &= rt + \frac{r^3t^3}{3!} + \frac{r^5t^5}{5!} + \frac{r^7t^7}{7!} + \cdots \\ &+ \frac{r^{2i+1}t^{2i+1}}{2i+1!} + \cdots + \cdots \\ &= \sum_{i=0}^{\infty} \frac{(rt)^{2i+1}}{2i+1!}, \end{aligned} \tag{3.1}$$

where $r \in N$ is a constant, and

$$\begin{aligned} &t^2 \sinh 2t \\ &= 2t^3 + \frac{2^3t^5}{3!} + \frac{2^5t^7}{5!} + \frac{2^7t^9}{7!} + \cdots \\ &\quad + \frac{2^{2i+1}t^{2i+3}}{2i+1!} + \cdots + \cdots \\ &= \sum_{i=0}^{\infty} \frac{2^{2i+1}t^{2i+3}}{2i+1!}. \end{aligned} \tag{3.2}$$

We allocated 0 to A and 1 to B then Z will be 25.

Let given message called plaintext be 'COMPUTER', it is equivalent to

2 14 12 15 20 19 4 17.

Let us assume that

$G_{0,0}=2,\quad G_{1,0}=14,\quad G_{2,0}=12,\quad G_{3,0}=15,\quad G_{4,0}=20,$

$G_{5,0}=19,\quad G_{6,0}=4,\quad G_{7,0}=17,\quad G_{n,0}=0$ for n $\geq$ 8.

Writing these numbers as a coefficients of $t^2\sinh 2t,$ and assuming $f(t)=Gt^2\sinh 2t,$ we get

$$f(t)=t^2[G_{0,0}2t+G_{1,0}\frac{2^3t^3}{3!}+G_{2,0}\frac{2^5t^5}{5!}$$
$$+G_{3,0}\frac{2^7t^7}{7!}+G_{4,0}\frac{2^9t^9}{9!}+G_{5,0}\frac{2^{11}t^{11}}{11!}$$
$$+G_{6,0}\frac{2^{13}t^{13}}{13!}+G_{7,0}\frac{2^{15}t^{15}}{15!}]$$
$$=\sum_{i=0}^{\infty}\frac{2^{2i+1}t^{2i+3}G_{i,0}}{2i+1!} \tag{3.3}$$
$$=2\frac{2t^3}{1!}+14\frac{2^3t^5}{3!}+12\frac{2^5t^7}{5!}+15\frac{2^7t^9}{7!}$$
$$+20\frac{2^9t^{11}}{9!}+19\frac{2^{11}t^{13}}{11!}+4\frac{2^{13}t^{15}}{13!}$$
$$+17\frac{2^{15}t^{17}}{15!}.$$

Taking Laplace transform on both sides we have

$$L\{f(t)\}=L\{Gt^2\sinh 2t\}$$
$$=\frac{24}{s^4}+\frac{2240}{s^6}+\frac{16128}{s^8}+\frac{138240}{s^{10}}$$
$$+\frac{1126400}{s^{12}}+\frac{6070272}{s^{14}}+\frac{6881280}{s^{16}} \tag{3.4}$$
$$+\frac{151519232}{s^{18}}.$$

Adjusting the resultant values

24 2240 16128 138240 1126400

6070272 6881280 151519232

to mod 26 that is

$$\begin{array}{ll} 24=24 \bmod 26, & 2240=4 \bmod 26, \\ 16128=8 \bmod 26, & 138240=24 \bmod 26, \\ 1126400=2 \bmod 26, & 6070272=0 \bmod 26, \\ 6881280=16 \bmod 26, & 151519232=20 \bmod 26. \end{array}$$

Sender sends the values

0 86 620 5316 43323

233472 264664 5827662

as a key. Assuming

$G_{0,1}=24,\quad G_{1,1}=4,\quad G_{2,1}=8,\quad G_{3,1}=24,$

$G_{4,1}=2\quad G_{5,1}=0,\quad G_{6,1}=16,\quad G_{7,1}=20,$

$G_{n,1}=0$ for n $\geq$ 8.

The given plain text gets converted to cipher text

24 4 8 24 2 0 16 20.

Here message 'COMPUTER' gets converted to 'YEIYCAQU'.

These results are included in the following

Theorem 3.1: *The given plain text in terms of* $G_{i,0},\ i=1,2,3,\cdots,$ *under Laplace transform of* $Gt^2\sinh 2t,$ *(that is by writing them as a coefficients of* $t^2\sinh 2t,$ *and then taking the Laplace transform) can be converted to cipher text*

$$G_{i,1}=2^{2i+1}(2i+2)(2i+3)G_{i,0} \bmod 26$$
$$=q_{i,1}-26k_{i,1},\quad for\ i=0,1,2,3,\cdots, \tag{3.5}$$

where,

$$q_{i,1}=2^{2i+1}(2i+2)(2i+3)G_{i,0},\ \ i=0,1,2,3,\cdots, \tag{3.6}$$

and a key

$$k_{i,1}=\frac{q_{i,1}-G_{i,1}}{26}\quad for\ i=0,1,2,3,\cdots. \tag{3.7}$$

Now we apply the same operation again on the output of the resulting cipher text obtained in the Theorem 3.1 and obtain its new form which is included in the following theorem.

Theorem 3.2: *The given plain text in terms of* $G_{i,1},\ i=1,2,3,\cdots,$ *under Laplace transform of* $G_{i,1}t^2\sinh 2t,$ *(that is by writing them as a coefficients of* $t^2\sinh 2t,$ *and then taking the Laplace transform) can be converted to cipher text*

$$G_{i,2}=G_{i,1}2^{2i+1}(2i+2)(2i+3)\bmod 26$$
$$=q_{i,2}-26k_{i,2},\ \ i=0,1,2,3,\cdots, \tag{3.8}$$

where,

$$q_{i,2}=G_{i,1}2^{2i+1}(2i+2)(2i+3),\ i=0,1,2,3,\cdots, \tag{3.9}$$

and a key

$$k_{i,2} = \frac{q_{i,2} - G_{i,2}}{26}, \ i = 0,1,2,3,\cdots, . \quad (3.10)$$

Now we apply such operations successively j times on the given plain text and obtain its new form as cipher text. This iterative method is included in the following theorem.

Theorem 3.3: *The given plain text in terms of* $G_{i,0}, \ i = 1,2,3,\cdots,$ *under Laplace transform of* $G_{i,0} t^2 \sinh 2t,$ *successively j times (that is by writing them as a coefficients of* $t^2 \sinh 2t,$ *and then taking the Laplace transform successively) can be converted to cipher text*

$$\begin{aligned} G_{i,j} &= G_{i,j-1} \ 2^{2i+1}(2i+2)(2i+3) \bmod 26 \\ &= q_{i,j} - 26k_{i,j}, \ i, j = 0,1,2,3,\cdots, \end{aligned} \quad (3.11)$$

where

$$\begin{aligned} &q_{i,j} = G_{i,j-1} 2^{2i+1}(2i+2)(2i+3), \\ &i, j = 0,1,2,3,\cdots, \end{aligned} \quad (3.12)$$

and a key

$$k_{i,j} = \frac{q_{i,j} - G_{i,j}}{26}, i, j = 0,1,2,3,\cdots, . \quad (3.13)$$

Remark 3.1: Theorem 3.1 is a special case of Theorem 3.3 with $j = 1$ and Theorem 3.2 with $j = 2$.

4. Generalization

The generalization of the results in section 3 can be obtained by considering more general function given by $f(t) = Gt^l \sinh rt, \ \ r, l \in N.$ Using the procedure discussed in section 3, we can convert the given message $G_{i,0}$ to $G_{i,1},$ where

$$\begin{aligned} q_{i,1} &= G_{i,0} r^{2i+1}(2i+2)(2i+3)\cdots(2i+l+1), \\ &\quad i, l = 0,1,2,\cdots, \end{aligned} \quad (4.1)$$

with key

$$k_{i,1} = \frac{q_{i,1} - G_{i,1}}{26}, \ i = 0,1,2,3,\cdots. \quad (4.2)$$

Hence we have following generalized theorem

Theorem 4.1: *The given plain text in terms of* $G_{i,0}, \ i = 1,2,3,\cdots,$ *under Laplace transform of* $G_{i,0} t^l \sinh rt,$ *(that is by writing them as a coefficients of* $t^l \sinh rt,$ *and then taking the Laplace transform) can be converted to cipher text*

$$\begin{aligned} G_{i,1} &= G_{i.0} \ r^{2i+1}(2i+2)(2i+3)\cdots \\ &\quad (2i+l+1) \ \bmod 26 \\ &= q_{i,1} - 26k_{i,1}, \ i, l = 0,1,2,3,\cdots, \end{aligned} \quad (4.3)$$

with $q_{i,1}$ *and* $k_{i,1}$ *are given by* (4.1) *and* (4.2) *respectively.*

Remark 4.1: Theorem 3.3 is a special case of theorem 4.1 with $l = 2, r = 2.$

Now we apply above operations successively j times on the output obtained in the last step on the cipher text and obtain new cipher text this is included in the following new theorem.

Theorem 4.2: *The given plain text in terms of* $G_{i,0}, \ i = 1,2,3,\cdots,$ *under Laplace transform of* $G_{i,0} t^l \sinh rt,$ *successively j times (that is by writing them as a coefficients of* $t^l \sinh rt,$ *and then taking the Laplace transform successively) can be converted to cipher text*

$$\begin{aligned} G_{i,j} &= G_{i,j-1} \ r^{2i+1}(2i+2)(2i+3)\cdots \\ &\quad (2i+l+1) \bmod 26 \\ &= q_{i,j} - 26k_{i,j}, \ i, j, l = 0,1,2,3,\cdots, \end{aligned} \quad (4.4)$$

and

$$\begin{aligned} q_{i,j} &= G_{i,j-1} r^{2i+1}(2i+2)(2i+3)\cdots \\ &\quad (2i+l+1), \ i, j, l = 0,1,2,3,\cdots, \end{aligned} \quad (4.5)$$

and key

$$k_{i,j} = \frac{q_{i,j} - G_{i,j}}{26}, \ i, j = 0,1,2,3,\cdots, . \quad (4.6)$$

Remark 4.1: Theorem 4.1 is a special case of Theorem 4.2 with $j = 1.$ Hence all Theorems 3.1 to 4.1 follows from Theorem 4.2.

5. Decryption

For the decryption of the received cipher text we proceed exactly in the reverse direction using inverse Laplace transform. The method is as follows.

Suppose we have received message as ‘YEIYCAQU’ which is equivalent to

$$24 \quad 4 \quad 8 \quad 24 \quad 2 \quad 0 \quad 16 \quad 20.$$

Let us assume that

Assuming

$G_{0,1} = 24$, $G_{1,1} = 4$, $G_{2,1} = 8$,

$G_{3,1} = 24$, $G_{4,1} = 2$ $G_{5,1} = 0$,

$G_{6,1} = 16$, $G_{7,1} = 20$, $G_{n,1} = 0$ for $n \geq 8$.

Using given key $k_{i,0},\ i = 0,1,2,3,\cdots$ as

0	86	620	5316
43323	233472	264664	5827662

and assuming

$$q_{i,1} = G_{i,1} + 26k_{i,1},\ i = 0,1,2,3,\cdots.. \tag{5.1}$$

We consider

$$\begin{aligned} &G\left(-\frac{d}{ds}\right)^2 \frac{2}{\left(s^2-2^2\right)} \\ &= \frac{24}{s^4} + \frac{2240}{s^6} + \frac{16128}{s^8} + \frac{138240}{s^{10}} \\ &\quad + \frac{1126400}{s^{12}} + \frac{6070272}{s^{14}} + \frac{6881280}{s^{16}} \\ &\quad + \frac{151519232}{s^{18}}. \\ &= \sum_{i=0}^{n} \frac{q_{i,1}}{s^{2i+4}}. \end{aligned} \tag{5.2}$$

Taking inverse Laplace transform we get

$$\begin{aligned} f(t) &= Gt^2 \sinh 2t \\ &= 2\frac{2t^3}{1!} + 14\frac{2^3t^5}{3!} + 12\frac{2^5t^7}{5!} \\ &\quad + 15\frac{2^7t^9}{7!} + 20\frac{2^9t^{11}}{9!} + 19\frac{2^{11}t^{13}}{11!} \\ &\quad + 4\frac{2^{13}t^{15}}{13!} + 17\frac{2^{15}t^{17}}{15!} \\ &= t^2[G_{0,0}.2t + G_{1,0}\frac{2^3t^3}{3!} + G_{2,0}\frac{2^5t^5}{5!} \\ &\quad + G_{3,0}\frac{2^7t^7}{7!} + G_{4,0}\frac{2^9t^9}{9!} + G_{5,0}\frac{2^{11}t^{11}}{11!} \\ &\quad + G_{6,0}\frac{2^{13}t^{13}}{13!} + G_{7,0}\frac{2^{15}t^{15}}{15!}]. \end{aligned} \tag{5.3}$$

Here we have

$G_{0,0} = 2$, $G_{1,0} = 14$, $G_{2,0} = 12$,

$G_{3,0} = 15$, $G_{4,0} = 20$, $G_{5,0} = 19$,

$G_{6,0} = 4$, $G_{7,0} = 17$, $G_{n,0} = 0$ for $n \geq 8$.

Here message 2 14 12 15 20 19 4 17 is equivalent to 'COMPUTER'.

Hence we have following

Theorem 5.1: *The given cipher text in terms of* $G_{i,1},\ i = 1,2,3,\cdots,$ *with a given key* $k_{i,0},\ i = 0,1,2,3,\cdots$ *can be converted to plain text* $G_{i,0}$ *under the inverse Laplace transform of*

$$G\left(-\frac{d}{ds}\right)^2 \frac{2}{\left(s^2-2^2\right)} = \sum_{i=0}^{n} \frac{q_{i,0}}{s^{2i+4}}, \tag{5.4}$$

where

$$G_{i,0} = \frac{26k_{i,0} + G_{i,1}}{2^{2i+1}(2i+2)(2i+3)},\ i = 0,1,2,3,\cdots, \tag{5.5}$$

and

$$q_{i,0} = 26k_{i,0} + G_{i,1},\ i = 0,1,2,3,\cdots. \tag{5.6}$$

The generalized iterative theorem can be obtained on the similar way which is included in the following

Theorem 5.2: *The given cipher text in terms of* $G_{i,j},\ i, j = 1,2,3\cdots,$ *with a given key* $k_{i,j-1},\ i, j = 1,2,3\cdots,$ *can be converted to plain text* $G_{i,j-1}$ *under the inverse Laplace transform of*

$$G\left(-\frac{d}{ds}\right)^2 \frac{2}{\left(s^2-2^2\right)} = \sum_{i=0}^{n} \frac{q_{i,j-1}}{s^{2i+4}}, \tag{5.7}$$

where

$$G_{i,j-1} = \frac{26k_{i,j-1} + G_{i,j}}{2^{2i+1}(2i+2)(2i+3)},\ i, j = 1,2,3,\cdots, \tag{5.8}$$

and

$$q_{i,j} = 26k_{i,j} + G_{i,j},\ i, j = 1,2,3,\cdots, \tag{5.9}$$

Remark 5.1: The most generalized decryption theorem corresponding to Theorem 4.2 can be obtained on the similar way.

Remark 5.2: Results in [7], G.Naga Lakshmi, B. Ravi Kumar and A. Chandra Sekhar are obtained by considering Laplace transform te^t and are generalized in [10, 11], Hiwarekar. Results in [4], Dhanorkar and Hiwarekar are obtained by using generalized Hill cipher algorithms.

4.1. Illustrative Examples

Using results obtained in Theorem 4.2, if we have original message 'COMPUTER', then it gets converted to

1. 'YMSYGAWG' for $r = 2, j = 3, l = 2,$
2. 'COOCUAEW' for $r = 2, j = 6, l = 2,$

3. ‘KOIQWAGU’ for $r = 3, j = 3, l = 3,$
4. ‘QMMKAAEA’ for $r = 5, j = 3, l = 4,$
5. ‘GOMGAAMA’ for $r = 5, j = 4, l = 4.$

6. Implementation Strategies

The main advantage of this algorithm is for same input alphabets we can get different output alphabets. We just need to change vale of ‘r’ or ‘j’ or both values (in theorem 4.2). Algorithm may prevent different attacks on the symmetric encryption such as ciphertext only, known plaintext, chosen plaintext, chosen ciphertext, chosen text. We can divide the document into blocks of four alphabets. Apply Encryption on these blocks in parallel and generate cipher text as well as the keys respectively. If we consider encryption of one complete document then we can choose different values of ′r′ (in Theorem 4.2) for different blocks. We can choose random function as follow:

$$r = rand()\%100$$

For each block chose different value of r so that by any way attacker cracked one block he will not be able to crack other blocks. We can also apply iterative method in some cases. This will resist all types of attacks mentioned earlier. For Brute Force attack large amount of calculations will be needed as attacker doesn’t know the algorithm as well as we are adding extra layer of security by using variable values of ‘r’ , ‘j’ or ‘l’ or all at a time (in Theorem 4.2). Other aspect of algorithm is key length it can be considered as advantage in some applications or disadvantage in case of data length limited applications.

7. Discussion and Concluding Remarks

1. For breaking a key of 256 bit by Bruce force attack, when faster super computer are used, it requires about $3:31 \times 10^{56}$ years, which is almost impossible

2. Many sectors such as banking and other financial institutions are adopting e-services and improving their Internet services. However, the e-service requirements are also opening up new opportunity to commit financial fraud. Internet banking fraud is one of the most serious electronic crimes and mostly committed by unauthorized users. The new method of key generation scheme developed in this paper may be used for a fraud prevention mechanism.

3. In the proposed work we develop a new cryptographic scheme using Laplace transforms and the key is the number of multiples of mod n. Therefore it is very difficult for an eyedropper to trace the key by any attack. The results in section 4 provide as many transformations as per the requirements which is the most useful factor for changing key.

4. The similar results can be obtained by using Laplace transform of a suitable function. Hence extension of this work is possible.

5. The entire document can be encrypted by considering block ciphers of small sizes.

6. For computer network security random number generation is a prime important task and also it is very essential in constructing keys for cryptographic algorithm. Method used in this paper can be useful for random number generation.

7. To reduce the crypt-analysis attack risk, a dynamic key theory plays important role the method presented in this paper is useful in such situations.

Acknowledgements:

Author is thankful to Principal Dr.S.B.Deosarkar and Vidya Pratishthan's College of Engineering, Baramati, Dist. Pune, Maharashtra, India, for the support to this work. Author is also thankful to BCUD University of Pune, India, for the financial support to this work under research project `Better network security using generalized Hill cipher algorithm'.

References

[1] Alexander Stanoyevitch, Introduction to cyrptography with mathematical foundations and computer implementations, CRC Press, (2002).

[2] Barr T.H., Invitation to Cryptography, Prentice Hall, (2002).

[3] Blakley G.R., Twenty years of Cryptography in the open literature, Security and Privacy 1999, Proceedings of the IEEE Symposium, 9-12, (May 1999).

[4] Dhanorkar G.A. and Hiwarekar A.P., A generalized Hill cipher using matrix transformation, International J. of Math. Sci. & Engg. Appls,Vol.5 No.IV, 19-23, (July2011).

[5] Eric C., Ronald K., James W.C., Netwark Security Bible Second edn.,Wiley India pub.(2009).

[6] Erwin Kreyszing, Advanced Engineering Mathematics,John Wiley and Sons Inc.(1999).

[7] G.Naga Lakshmi, B.Ravi Kumar and A.Chandra Sekhar, A cryptographic scheme of Laplace transforms, International Journal of Mathematical Archive-2, 2515-2519, (2011).

[8] Grewal B.S., Higher Engineering Mathematics, Khanna Pub., Delhi, (2005).

[9] Gupta P., Mishra P. R., Cryptanalysis of “A New Method of Cryptography Using Laplace Transform, Proceedings of the Third International Conference

on Soft Computing for Problem Solving Advances in Intelligent Systems and Computing Vol.258, 2014, 539-546.

[10] Hiwarekar A.P., A new method of cryptography using Laplace transform, International Journal of Mathematical Archive, 3(3), 1193-1197, (2012).

[11] Hiwarekar A.P., A new method of cryptography using Laplace transform of hyperbolic functions, International Journal of Mathematical Archive, 4(2), 208-213, (2013).

[12] Johannes A. Buchmann, Introduction to Cryptography,Fourth Edn.,Indian Reprint , Springer, (2009).

[13] Lokenath Debnath, Dambaru Bhatta, Integrl Transforms and Their Applications, Chapman and Hall/CRC,First Indian edn.(2010).

[14] Overbey J., Traves W.and Wojdylo J., On the Keyspace of the Hill Cipher, Cryptologia, 29, 59-72, (January 2005).

[15] Ramana B.V., Higher Engineering Mathematics, Tata McGraw-Hills, (2007).

[16] Saeednia S., How to Make the Hill Cipher Secure, Cryptologia, 24, 353-360, (October 2000).

[17] Stallings W., Cryptography and network security, 4th edition, Prentice Hall, (2005).

[18] Stallings W., Network security essentials: Applications and standards, first edition, Pearson Education, Asia, (2001).

[19] Sujitha S., Applications of Laplace Transforms in Cryptography, International Journal of Mathematical Archive, 4(3), 2013, 67-71.

[20] Sukalyan S., Moumita S., DNA Secret Writing With Laplace Transform, International Journal of Computer Applications, Vol. 50 – No.5, July 2012, 44-50.

[21] Vyavahare S., Bani Upmanayu, A, Cryptographic Scheme using Infinite Series and Laplace transform, Global Research Analysis,Vol.2, No.6 June 2013, 60-61.

Anil P Hiwarekar obtained M.Sc., M.Phil. (Mathematics) and has extended his M.Phil. work for his Ph.D. on ‘Elliptic and Parabolic boundary value problems with applications’. He has been awarded Ph.D. degree in 2008 from Dr.B.A.M.University, Aurangabad, Maharashtra, India. Anil has twenty five years teaching experience at undergraduate and postgraduate level. He is working in Vidya Pratishthan’s College of Engineering Baramati from March 2001. Anil also has to his credit sixteen publications out of which four research papers are published in the International Journals and four in National Journals. He has presented eleven papers in International and National Conferences. He has attended around twenty one workshops/ conferences/ Seminars and also attended seven summer /refresher courses. He has an important role in organizing about twelve conferences/ workshops / programs. He was a chairman of one session of AMTI National Conference (Dec.2011) at Baramati. He is working on BCUD Research project ‘Better Network Security Using Generalized Hill Cipher Algorithm'. Sanctioned by University of Pune, Maharashtra, India.

He is a life member of ISTE, Marathwada Mathematical Society, Aurangabad and All India Mathematics Teachers of India. He is also member of international association of Engineers.